UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF VARIOUS ELECTRONIC DEVICES WHICH ARE STORED AT THE KNOX COUNTY SHERIFF'S OFFICE, 11540 UPPER GILCHRIST ROAD, MOUNT VERNON, OHIO, SPECIFICALLY: BLACK APPLE IPHONE LIGHT BLUE APPLE IPHONE LIGHT PURPLE APPLE IPHONE APPLE LAPTOP (S/N: CO2FXF1MMD6M / MODEL: A2141) TIGER DASH CAM (FCCID: 2A2ME-F7N / MODEL: F7NP)	**CASE NO.** 2:23-mj-699

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, J. Michael McClelland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a series of electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a U.S. Postal Inspector with the U.S. Postal Inspection Service ("USPIS"), stationed in Columbus, Ohio, and have been since March 2015. My responsibilities include

investigating money laundering, financial crimes, identity theft, mail theft, mail fraud, bank fraud, intellectual property fraud, prohibited mailings, dangerous mail, and other violations with a nexus to the U.S. Postal Service. Prior to becoming a U.S. Postal Inspector, I was a Special Agent with the U.S. Secret Service from December 2002 through March 2015. My responsibilities as a Special Agent included investigating financial crimes, identity theft, counterfeit currency, bank fraud, wire fraud, access device fraud, and threats against the President and Vice President of the United States. I have received initial and follow-up law enforcement training throughout my career as a U.S. Postal Inspector and U.S. Secret Service Agent. This training included the seizure and examination of electronic devices in connection with federal investigations.

3. This affidavit based on my own personal involvement in this investigation, as well as information that I have obtained from other law enforcement officers, to include the execution of State of Ohio search warrants. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched consists of the following electronic devices (hereinafter, "the Devices"), which were all seized on December 1, 2023, from a vehicle parked on Devore Road, Mount Vernon, OH, near the intersection of Devore Road and Morgan Center Road, Mount Vernon, OH. The vehicle and occupants were identified as being associated with a scheme to defraud. Below is a list of the devices:

a. Black Apple iPhone in $100 bill case
b. Light blue Apple iPhone in Blane & Eclare glitter case

c. Light purple Apple iPhone in black case with white markings
d. Apple Laptop Computer, S/N: CO2FXF1MMD6M / Model: A2141
e. Dash Camera, FCCID: 2A2ME-F7N / Model: F7NP

The Devices are all currently located at the Knox County Sheriff's Office, 11540 Upper Gilchrist Road, Mount Vernon, Ohio.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. This investigation centers on a scheme to defraud the victim out of money through use of deceptive phone calls. Receipts for U.S. Postal Money Orders were recovered from the vehicle, along with receipts for U.S. Express mailings, which is indicative of money laundering using the U.S. Mail. In addition, $86,537 along with a ledger with various addresses written in it were recovered from the vehicle.

7. On or about November 30, 2023, victim G.H. reported to the Knox County Sheriff's Office that a pop-up appeared on the computer stating that the computer had been hacked and now has a virus. In addition, a phone number was displayed on the computer screen.

8. G.H. contacted the phone number that was displayed on the computer screen and was told by an unknown individual that G.H.'s computer has been hacked. The unknown individual discussed computer programs with G.H. and then asked G.H. to input bank account information. The unknown individual then attempted to get G.H. to open a bank account. The unknown individual then asked G.H. to provide the name of the bank that G.H. has an account with. G.H. was provided with another phone number to contact regarding the supposed computer hack and virus.

9. G.H. contacted the provided phone number and spoke to an individual claiming to be John Harper from G.H.'s local bank. G.H. was then instructed to contact another phone number.

10. G.H. contacted the provided phone number and spoke to an individual claiming to be an associate of the Social Security Administration (SSA). The SSA associate informed G.H. that the FBI is now involved and there are illegal images on G.H.'s computer. The SSA associate told G.H. that $30,000 needed to be paid to resolve the issue on the computer. G.H. was instructed to withdraw $30,000 and place it in a box. G.H. was told that an FBI agent would come to G.H.'s residence on December 1, 2023, between the hours of 8:30-9:30AM to retrieve the box of money.

11. On or about December 1, 2023, G.H. received a phone call from one of the unknown individuals that G.H. spoke to on November 30, 2023. The unknown individual advised G.H. that the FBI agent is in enroute to G.H.'s residence to pick up the money. The unknown individual advised G.H. to go outside and hand the box to the FBI agent and say the code word "Blue". The unknown individual advised G.H. he would place the call on hold and that he needed to contact the FBI agent to get her location. Knox County Sheriff deputies were present at G.H.'s residence at the time of the call and advised G.H. to place the box on the vehicle parked in G.H.'s driveway. The unknown individual returned to the call and advised G.H. that the FBI agent was a female and that she would be wearing a sweater, with black and white pants that had flowers on them. The unknown individual again advised G.H. to go outside and hand the box to the FBI agent. G.H. advised that the box was placed on the vehicle in G.H.'s driveway and could be picked up by the FBI agent.

12. Continuing this date, a female fitting the above description arrived at G.H.'s residence and stood in the driveway approximately 10 feet from the front door of G.H.'s residence. Knox County Sheriff deputies observed the female on a cell phone in G.H.'s driveway. The female then began to walk away from the residence when Knox County Sheriff deputies detained her. The female was identified as Huan Liu.

13. Continuing this date, Knox County Sheriff deputies observed a Hyundai Palisade bearing a Wisconsin license plate ASZ7758, parked with its hazard lights flashing near G.H.'s residence. The occupants of the vehicle were identified as Zhuxian Min and Jingchen Li. The above vehicle is registered to Min. Min told Knox County Sheriff deputies that he was giving Lui a ride. Min gave Knox County Sheriff deputies consent to search the vehicle. During the consent search of the vehicle Knox County Sheriff deputies found three (3) Apple iPhones, one (1) Apple laptop computer, electric money counter, ledger that contained addresses with money amounts written next to the addresses, personal items, money bands, USPS mail receipts, USPS money order receipts, identification documents, dash camera and $86,537 US currency. The Knox County Sheriff's Office then made contact with the Knox County Prosecutor's Office. The Knox County Prosecutor's Office advised that all three subject be placed under arrest and the vehicle be impounded.

14. The Devices currently remain in the lawful possession of the Knox County Sheriff's Office, at 11540 Upper Gilchrist Road, Mount Vernon, Ohio. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Knox County Sheriff's Office.

15. Although the Knox County Sheriff's Office might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cell phone: A cell phone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other cell phones or traditional "land line" telephones. A cell phone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cell phones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cell phones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated

"GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178).

Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that several of the Devices have capabilities that allow them to serve as a cell phone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. Based on the facts set forth in this Affidavit, I maintain there is probable cause to believe that there is evidence regarding the activities described above, in violation of Title 18, United States Code, Section 1341 (mail fraud); Section 1343 (wire fraud); and Section 1956 (conspiracy to commit money laundering), located in the items listed on Attachment A, as described in particularity in Attachment B.

24. Accordingly, I respectfully request that the Court issue a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

J. Michael McClelland
United States Postal Inspector

Subscribed and sworn to before me
on December 18, 2023:

Chelsey M. Vascura
United States Magistrate Judge

ATTACHMENT A
(Property to Be Searched)

The property to be searched ("the Devices"), described below, was all seized in connection with a search incident to arrest by the Knox County Sheriff's Office on December 1, 2023, at the victim G.H.'s residence and from the above described Hyundai Palisade, bearing Wisconsin license plate ASZ7758, which was parked at the intersection of Devore Road and Morgan Center Road, Mount Vernon, OH. The Devices are currently located at the Knox County Sheriff's Office, 11540 Upper Gilchrist Road, Mount Vernon, Ohio.

a. Black Apple iPhone in $100 bill case;

b. Light blue Apple iPhone in Blane & Eclare glitter case;

c. Light purple Apple iPhone in black case with white markings;

d. Apple Laptop Computer, S/N: CO2FXF1MMD6M / Model: A2141;

e. Dash Camera, FCCID: 2A2ME-F7N / Model: F7NP;

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMEBT B
(Items to Be Seized)

1. All records since June 1, 2023, on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 1341 (mail fraud), § 1343 (wire fraud), or § 1956 (conspiracy to commit money laundering) by Huan Liu, Zhuxian Min, Jingchen Li, or their coconspirators (the "Subjects"), including:

a. Any records relating to U.S. Mail Parcels, U.S. Postal Service Informed Delivery, and U.S. Mail Carrier Information, including text messages, photographs, cell phone application data;

b. lists of customers/victims and related identifying information, including records related to G.H.;

c. types, amounts, and prices of credit/debit/gift cards, as well as dates, places, and amounts of specific transactions and travel records;

d. any information related to sources of victims' personal identifying information (including names, addresses, phone numbers, or any other identifying information);

e. any information and communications among or relating to Subjects, including contact lists, written or recorded communications, and images or videos;

f. any information relating to the schedule, travel, or location of any of the Subjects;

g. any records of Internet and computer activity, including firewall logs, caches, browser history and cookies, "bookmarked" or favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

h. any digital records or recordings found on the dash camera (including videos and images that evidence routes, identities, sources of the other evidence found in the car, and the execution of the scheme);

i. all bank records, storage unit records, safe deposit box records, stored value cards, credit cards, checks, credit card bills, account information, and other financial records;

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the U.S. Postal Inspection Service may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.